Certification Authorities

presented to

ADPO

John Volmer

Electronics and Computing Technologies Division

November 13, 1996

Signature Examples

- Purchase Requisition
- Memoranda

Signature Characteristics

- The signature identifies the signer
  - Typically it is eye-readable
  - Often across organizational boundaries
- The signature is unique
  - Only the owner of the signature can create that mark
- The signature cannot be duplicated
  - No two people have the same signature

Signature Characteristics (Cont.)

- The document is unalterable
  - A field cannot be changed
  - A field cannot be added
  - A field cannot be removed
  - without the change being detectable

Signature Capability

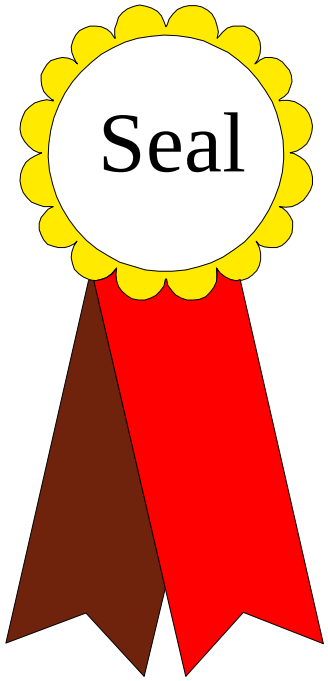
- Because of these characteristics, a signature is legally binding
- In effect, it is non-repudiatable
  - You can't say you didn't sign it

Electronic Signature Problem

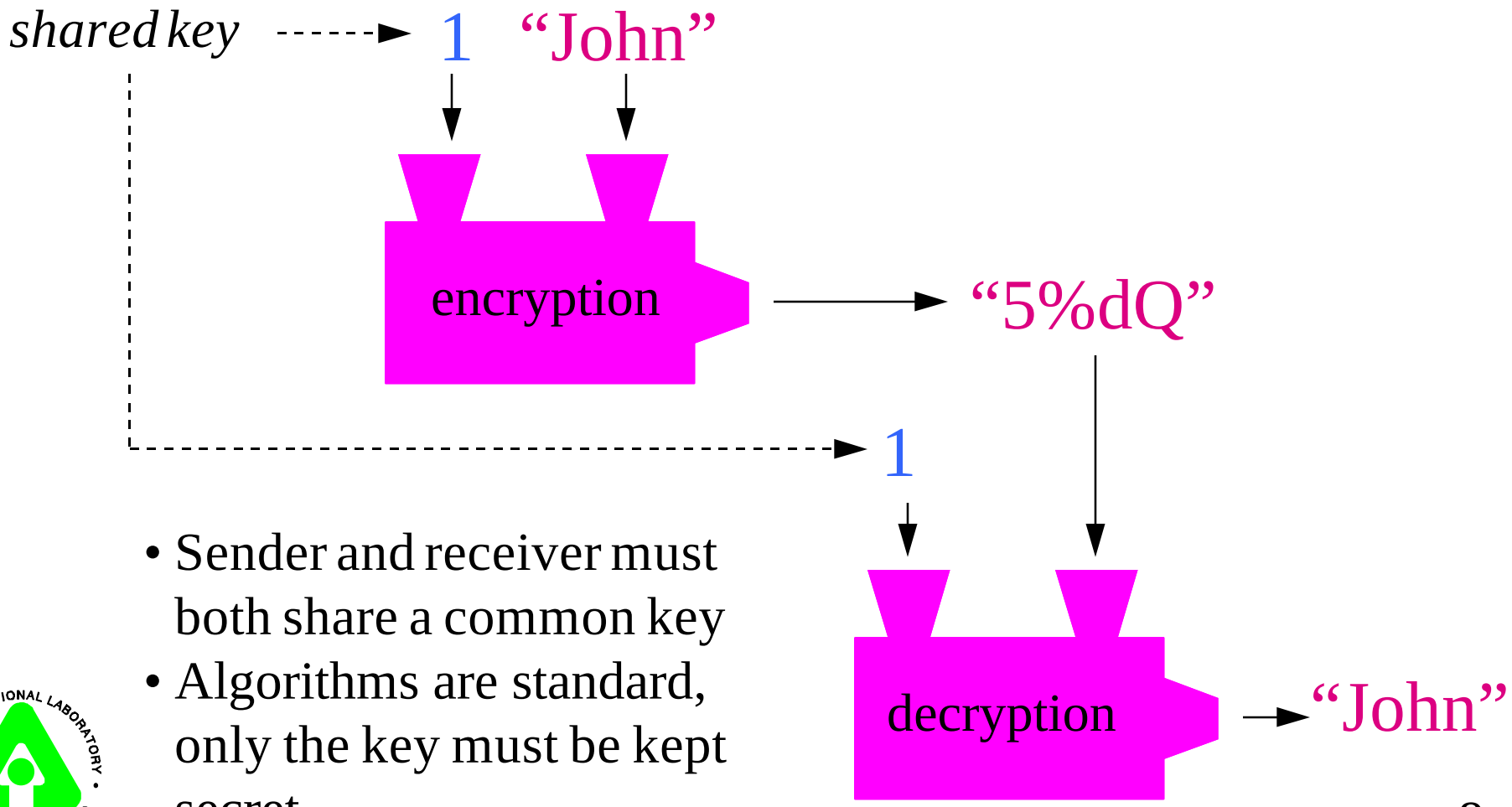
- How do you provide the same characteristics as a physical signature, when every bit is potentially dynamic?
  - How do you uniquely tie a person to a digital symbol?
  - Computers have no trouble copying data
  - Computers are discreet machines; it is easy for independent people to duplicate simple bit patterns
  - Computers change data continuously

Conceptually

- In the past
  - People have relied on wax seals to authenticate
  - They used encryption to hide the contents
- Today we do the same thing
  - We use encryption to affix a seal to a document
  - We use encryption to hide the contents of a document

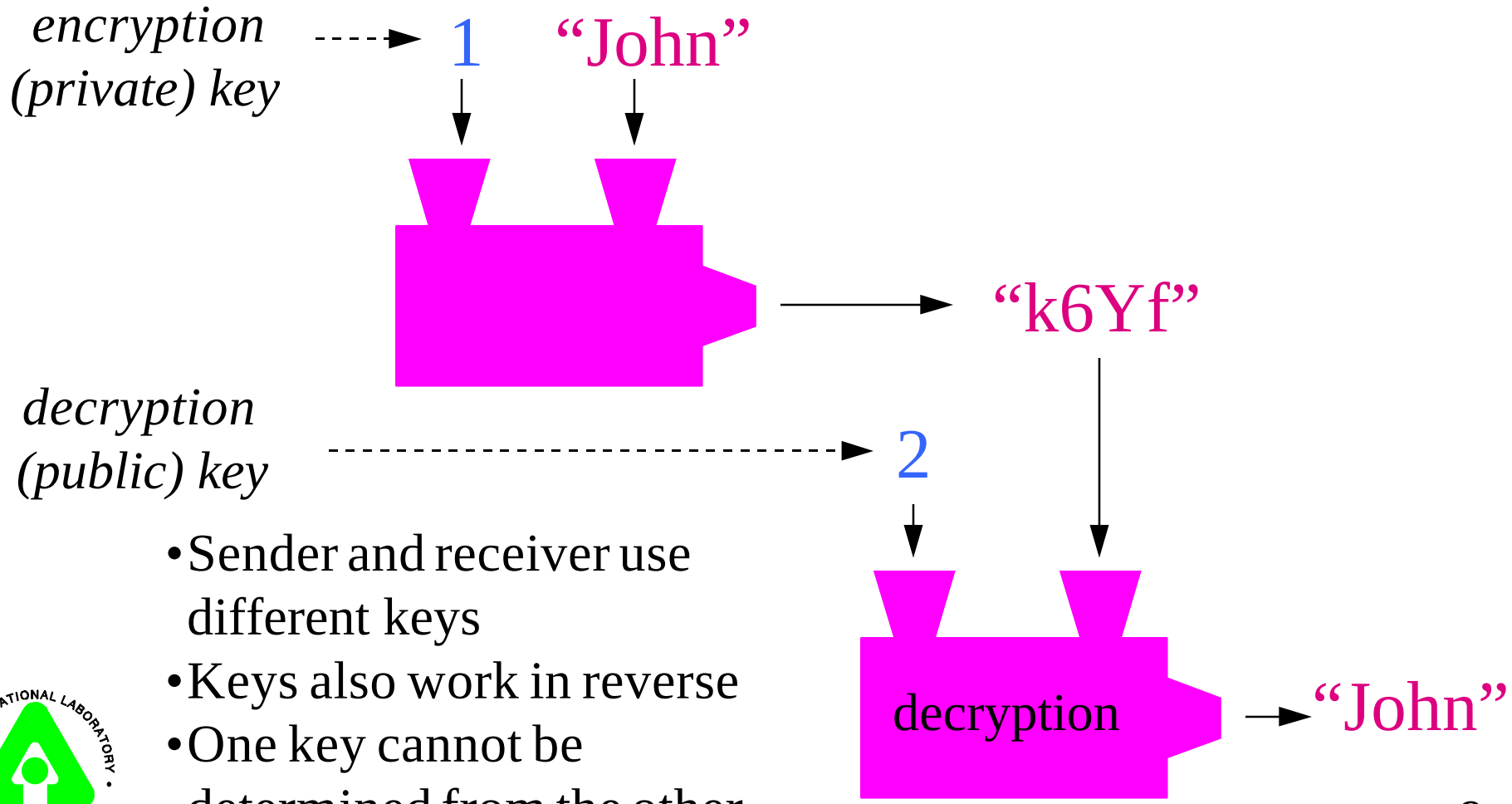


Private Key (Symmetric) Encryption



- Sender and receiver must both share a common key
- Algorithms are standard, only the key must be kept secret

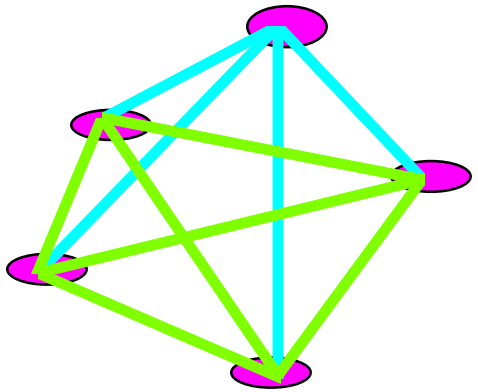
Public/Private Key (Asymmetric) Encryption



- Sender and receiver use different keys
- Keys also work in reverse
- One key cannot be determined from the other

Private Key Characteristics

- It is easier to understand
- It is computationally faster
- But, it does not scale . . .

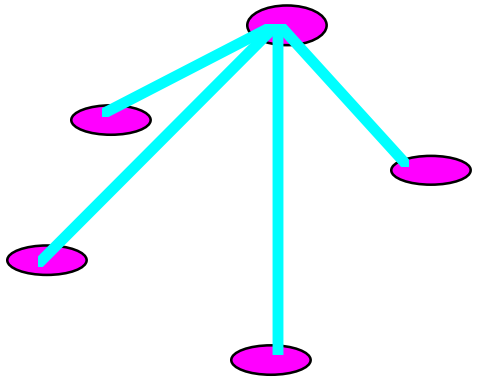


Order N^2

- You must exchange a key pair with all of your partners in advance

Public Key Characteristics

- Harder to understand
- Computationally more difficult
- But, it scales !



Order *N*

- You only need to announce your public key once

How Does Public/Private Key Provide a Signature?

- The signature identifies the signer
  - The public key is recorded in a database with the identity of the owner
  - Only the public key can decrypt private key encrypted material
  - Hence, it can verify material encrypted by a user's private key

How Does Public/Private Key Provide a Signature? (Cont.)

- The signature is unique
  - It is a big number
  - 1024 binary digits, or
  - 128 characters, or
  - 256^{128} possible combinations

100101011101 . . . 011110110110

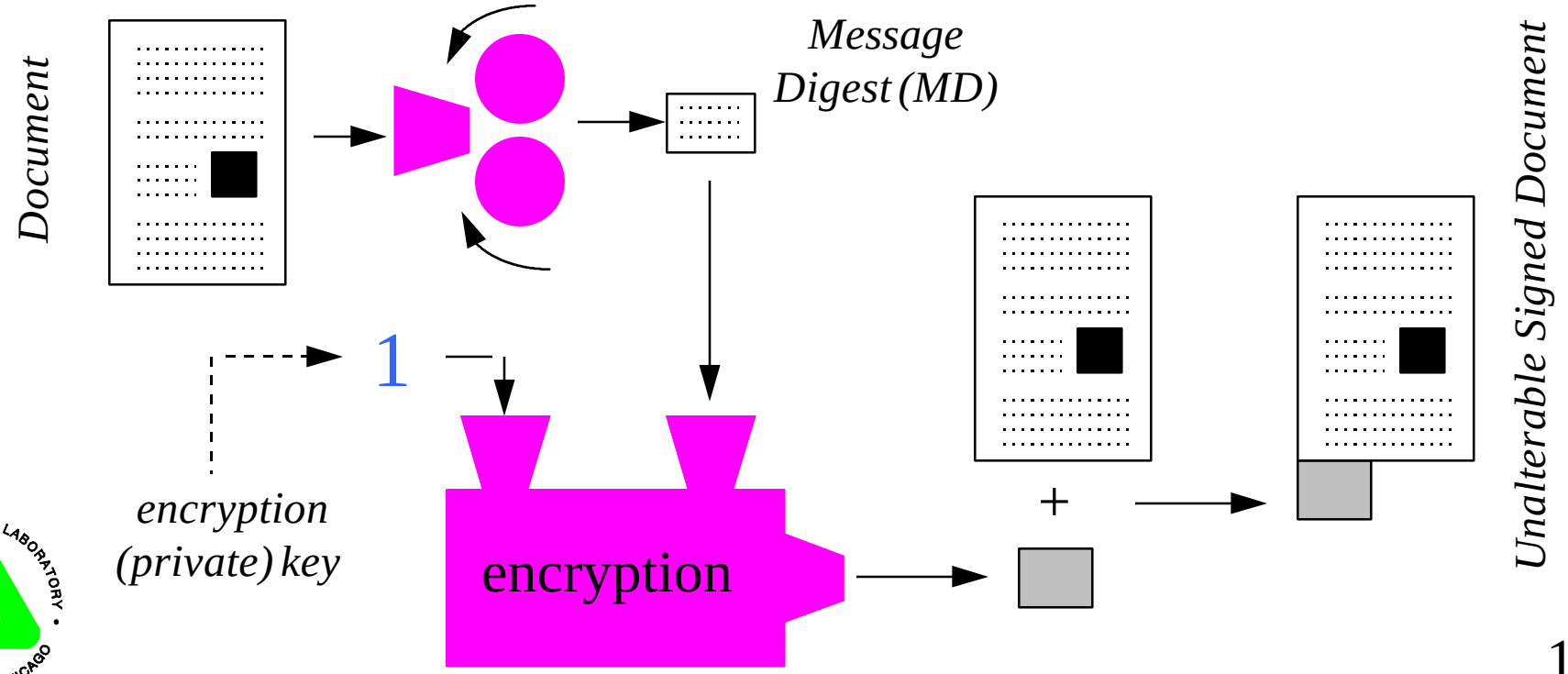
1024 digits

How Does Public/Private Key Provide a Signature? (Cont.)

- The signature cannot be duplicated
  - It is virtually impossible to duplicate randomly
  - The public and private keys are precisely related mathematically; no other key will decode a private key encryption

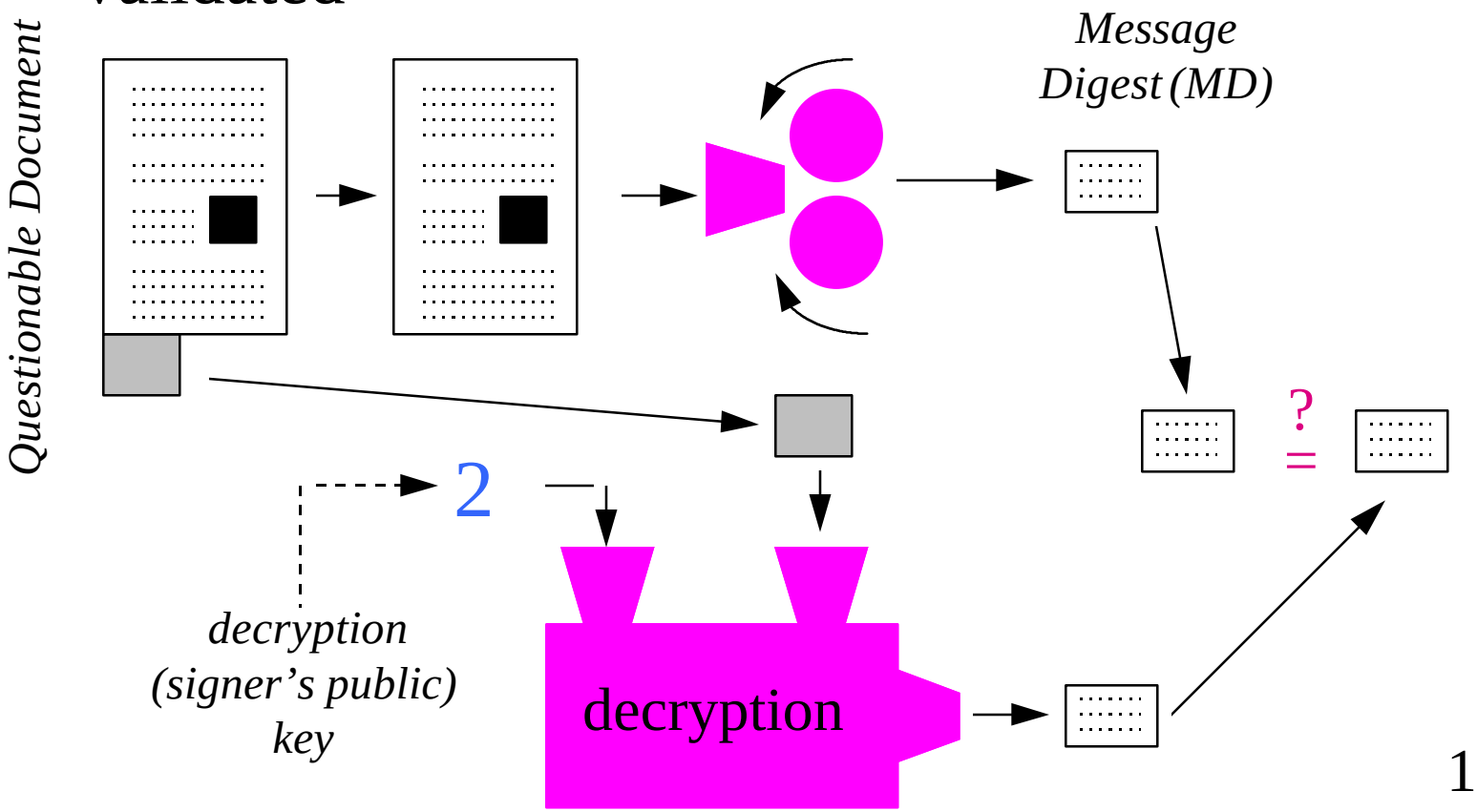
How Does Public/Private Key Provide a Signature? (Cont.)

- The document is unalterable
  - A message digest is appended to the document



How Does Public/Private Key Provide a Signature? (Cont.)

- The message digest can be subsequently validated



So, What Does a CA Have To Do With All This?

- First, it computes the public/private key pair
  - Not a trivial task for such big numbers
  - Ensures that key pairs are unique

So, What Does a CA Have To Do With All This? (Cont.)

- Second, it is a trusted party that tells others what the public key for a user is
  - Keeps track of who owns which public key
  - Essential for identifying the signer
    - If you receive a document from Carol Quinn how do determine what her public key is?
    - *Answer*: you ask Carol's CA to provide a X.509 V3 certificate stating her identity and her public key

So, What Does a CA Have To Do With All This? (Cont.)

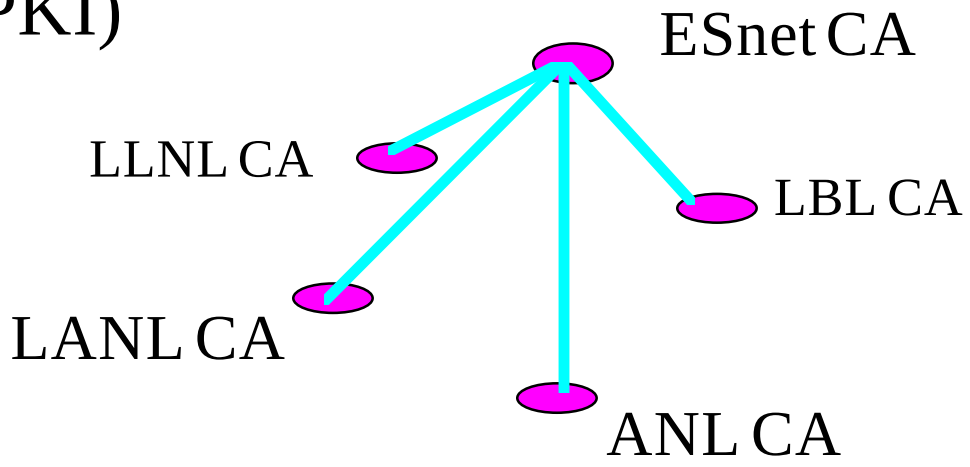
- Thirdly, it handles private keys that have been compromised
  - Earlier I said that these keys are so big that the signature is unique
  - However, a user or CA failure could divulge a user's private key, thus allowing duplication
  - The CA keeps a list of private keys that have been compromised
  - It provides this list to other applications that need to validate signatures

. . . it is a trusted party . . .

- What does it mean to trust a CA?
  - How well do I have to manage my CA for it to be trustworthy?
  - What must Carol Quinn do to prove her initial identity to the CA?
  - If a CA turns out not to be trustworthy, is anyone liable?
  - Extensive discussions are underway to define trust.

. . . you ask Carol's CA . . .

- If the user whose signature you want to verify is from another organization, how do you determine where Carol's CA is?
  - *Answer:* You use the Public Key Infrastructure (PKI)



- But that is another presentation . . .

Reasons for establishing a CA at ANL

- Enables digital signature applications
- Enables participation in the national PKI
- Enables participation in the federal PKI
- Enables ANL to perform public/private key authentication
- Enables ANL to issue X.509 V3 certificates

Certification Authorities

- For more information see http://www.anl.gov/ECT/certify
- Questions?